



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/584,864	06/28/2006	Manuel Leone	09952.0067	7895
22852	7590	03/26/2010	EXAMINER	
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP 901 NEW YORK AVENUE, NW WASHINGTON, DC 20001-4413				CHEN, SHIN HON
ART UNIT		PAPER NUMBER		
2431				
			MAIL DATE	DELIVERY MODE
			03/26/2010	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/584,864	LEONE ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	SHIN-HON CHEN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 23 March 2010.  
 2a) This action is **FINAL**.                    2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 24-41 and 43-46 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 24-41 and 43-46 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on 23 March 2010 is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) <input type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____ .
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.	5) <input type="checkbox"/> Notice of Informal Patent Application
	6) <input type="checkbox"/> Other: _____ .

## **DETAILED ACTION**

1. Claims 24-41 and 43-46 have been examined.

### ***Continued Examination Under 37 CFR 1.114***

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 3/23/10 has been entered.

### ***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 24-41 and 43-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ben-Chuan et al. U.S. Pat. No. 7177425 (hereinafter Ben) in view of Campbell U.S. Pub. No. 20040204124 (hereinafter Campbell).

5. As per claim 24, Ben discloses a method for the cipher controlled exploitation of data resources stored in a database associated with a computer system, comprising the steps of: providing a subscriber identity module carrying at least one security algorithm (Ben: column 3

lines 28-31: the cipher key generating module is SIM); producing a cipher key via said at least one security algorithm, said subscriber identity module not used by said computer system for communication with a network (Ben: column 3 lines 28-31: the SIM card is used to generate cipher keys for encryption, not directly used for communication with a network); and using said cipher key for protecting said data resource (Ben: column 2 lines 30-35). Ben does not explicitly disclose a remote storing location accessible by said user via a communications network.

However, Campbell discloses a remote server database that allows users of portable or wireless devices to store personal information/file in the database over a network (Campbell: [0004]). It would have been obvious to one having ordinary skill in the art to allow users to encrypt user's private/personal information and store in a wireless device and upload the desired encrypted files to remote server database for storage because both devices are capable of performing communication over network. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Campbell within the system of Ben because it provides greater amount of memory space through remote server database.

6. As per claim 25, Ben discloses the method according to claim 24. Ben further discloses wherein said step of using said cipher key for protecting said data resources comprises the steps of: encrypting said data resources by means of said cipher key (Ben: column 2 lines 30-35); storing encrypted data resources in storage and retrieve encrypted resources from storage for decryption (Ben: column 5 lines 26-38).

Ben does not explicitly disclose a remote storing location accessible by said user via a communications network. However, Campbell discloses a remote server database that allows users of portable or wireless devices to store personal information/file in the database over a network (Campbell: [0004]). It would have been obvious to one having ordinary skill in the art to allow users to encrypt user's private/personal information and store in a wireless device and upload the desired encrypted files to remote server database for storage because both devices are capable of performing communication over network. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Campbell within the system of Ben because it provides greater amount of memory space through remote server database.

7. As per claim 26, Ben discloses the method according to claim 24. Ben further discloses wherein said step of producing a cipher key comprises the steps of: generating at least one random value; subjecting said at least one random value to said at least one security algorithm to generate at least one session key; and processing said at least one session key via a mixer function to produce said at least one cipher key (Ben: column 2 lines 1-2: providing cipher key; column 5 lines 4-15: generating cipher key based on random values).

8. As per claim 27, Ben discloses the method according to claim 26. Ben further discloses the steps of: generating at least two random values; subjecting said at least two random values to said at least one security algorithm to generate at least two session keys; and combining said at

least two session keys via a mixer function to produce said at least one cipher key (Ben: column 5 lines 4-15).

9. As per claim 28, Ben discloses the method according to claim 26. Ben further discloses wherein said mixer function comprises a hash function (Ben: column 5 lines 21-25).

10. As per claim 29, Ben discloses the method according to claim 26. Ben further discloses the step of inserting in said mixer function a user specific secret unrelated to said subscriber identity module security algorithm, whereby said cipher key is unpredictable even based on knowledge of said security algorithm carried in said subscriber identity module (Ben: column 3 lines 28-37).

11. As per claim 30, Ben discloses the method according to claim 24. Ben further discloses the step of selecting said data resources from user sensitive data or user credentials (Ben: column 4 lines 21-28).

12. As per claim 31, Ben discloses the method according to claim 30. Ben further discloses wherein said step of using said cipher key for protecting said data resources comprises the step of encrypting by means of said cipher key, said user sensitive data or said user credentials from plain text into an encrypted format (Ben: column 2 lines 29-35).

13. As per claim 32, Ben discloses the method according to claim 31. Ben further discloses wherein said step of using said cipher key for protecting said data resources comprises the step of decrypting by means of said cipher key said user sensitive data or said user credentials from an encrypted format into plain text (Ben: column 6 lines 21-24).

14. As per claim 33, Ben discloses the method according to claim 31. Ben further discloses wherein said user sensitive data or said user credentials in encrypted format have a cryptographic header associated therewith (Ben: column 5 lines 26-38).

15. As per claim 34, Ben discloses the method according to claim 33. Ben further discloses wherein said cryptographic header comprises an identifier of said subscriber identity module and a cryptographic checksum based on said cipher key, said cryptographic checksum being used for detecting any unauthorized modifications of said encrypted format (Ben: column 5 lines 21-25).

16. As per claim 35, Ben discloses the method according to claim 30. Ben does not explicitly disclose wherein said data resources are user credentials, said database associated with said computer system is a remote database and said data resources based on said user credentials are stored in said remote database in an encrypted format. However, Campbell discloses a remote server database that allows users of portable or wireless devices to store personal information/file in the database over a network (Campbell: [0004]). It would have been obvious to one having ordinary skill in the art to allow users to encrypt user's private/personal information and store in a wireless device and upload the desired encrypted files to remote server database for storage

because both devices are capable of performing communication over network. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Campbell within the system of Ben because it provides greater amount of memory space through remote server database.

17. As per claim 36, Ben as modified discloses the method according to claim 35. Ben as modified further discloses the step of establishing a relationship between said user credentials stored in said encrypted format in said remote database and a corresponding user subscriber identity module (Campbell: [0004]).

18. As per claim 37, Ben as modified discloses the method according to claim 36. Ben as modified further discloses wherein said relationship is established by means of an identifier of said subscriber identity module (Campbell: [0004]).

19. As per claim 38, Ben as modified discloses the method according to claim 37. Ben as modified further discloses the step of using said identifier for searching within said remote database to permit said user exploitation of said user credentials (Campbell: [0004]).

20. As per claim 39-46, claims 39-46 encompass the same scope as claims 24-38. Therefore, claims 39-46 are rejected based on the same reason set forth above in rejecting claims 39-46.

***Response to Arguments***

21. Applicant's arguments filed 3/23/10 have been fully considered but they are not persuasive.

Regarding applicant's remarks, applicant mainly argues that the prior art of record does not explicitly disclose that the SIM card is not used by computer system for communication with a network. However, the examiner disagrees. Ben discloses that the SIM is a cipher key generating module, although it encrypts data to be stored at another location, it is not directly used for communication with a network (Ben: column 3 lines 28-31). Therefore, applicant's argument is not persuasive in light of above explanation. Applicant is welcome to contact the examiner to discuss claim language to expedite prosecution.

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHIN-HON CHEN whose telephone number is (571)272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shin-Hon Chen  
Primary Examiner  
Art Unit 2431

/Shin-Hon Chen/  
Primary Examiner, Art Unit 2431